



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,906	12/28/2001	Nicholas Paul Kelly	01.103.01	2851
7590	11/13/2006		EXAMINER	
Zilka-Kotab, PC P.O. Box 721120 San Jose, CA 95172-1120			LAFORGIA, CHRISTIAN A	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 11/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

NOV 13 2006

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/028,906

Filing Date: December 28, 2001

Appellant(s): KELLY ET AL.

Kevin Zilka
Reg. No. 41,429
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 28 August 2006 appealing from the Office action mailed 18 January 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

NEW GROUND(S) OF REJECTION

Claims 27-39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,886,099	SMITHSON et al.	04-2005
6,401,210	TEMPLETON	06-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-13 and 27-39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As per claims 1-13, merely claimed as a computer program product comprising various code modules representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical “thing” nor a statutory process, as there are not “acts” being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program product and other claimed aspects of the invention which permit the computer program’s functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program’s functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program’s functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31 USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

As per claims 27-39, merely claimed as an apparatus comprising various logic modules representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical “thing” nor a statutory process, as there are not “acts” being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program product and other claimed aspects of the invention which permit the computer program’s functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program’s functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program’s functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31 USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

Claims 1, 2, 7-12, 14, 15, 20-25, 27, 28, and 33-38 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,711,583 to Chess et al., in view of U.S. Patent No. 6,886,099 to Smithson.

As per claims 1, 14 and 27, Chess discloses a computer program product for operating a computer to review files for potential malware (column 4, lines 4-10), comprising:
logging code operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of

times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file (column 4, line 62 through column 5, line 5, i.e. maintaining in the database the Nth occurrence of the document being scanned);

statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file (column 2, lines 44-54, column 5, lines 11-16);

action determination code operable, if the count value determined by the statistical log interface code exceeds a predetermined threshold (column 6, lines 15-28).

Chess does not disclose a weighting table identifying, for each value of the predetermined attributes, a weighting indicating the likelihood that a file having that value of predetermined attributes will be malware and to reference the weighting table to determine the weighting to be associated with the file in case the count value exceeds the threshold and take actions based on that weight.

Smithson discloses a method for computer virus detection where he discloses a method for detecting computer viruses based on some predetermined criteria such as the count of the file (See Abstract) where he teaches using a weighting table identifying, for each value of predetermined attributes (column 4, lines 50- 62, column 9, lines 21-27), a weighting indicating the likelihood that a file having that value of said one or more predetermined attributes will be malware (column 4, lines 5-20), based on the value of said one or more predetermined attributes associated with that file in the statistical log (column 4, lines 25-40, column 6, lines 35-43), and performing a predetermined actions dependent on the weighting determined by determination code (column 6, lines 34-44 and column 8, lines 13-31).

It would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Chess system with the teachings of Smithson to base actions based on a weighting tables for the files. One would be motivated to do so in order to enable the system to detect unknown viruses, because using such technique is not looking for an individual virus or pattern of execution of a virus, it is able to more readily detect previously unknown viruses by the effect that they have on the activity of the computer system as a whole (Smithson: column 2, lines 10-15).

Regarding claims 2, 15 and 28, Chess wherein said one or more predetermined attributes comprise an indication of the file type of the file (column 4, lines 24-34).

Regarding claims 7, 20 and 33, Chess discloses wherein if the weighting indicates that the file is to be treated with caution, said action performing code is operable to perform the steps of:

- (i) associating a warning message with the file for reference by a person receiving that file (column 5, lines 39-46, i.e. "questionable" status), and
- (ii) generating for access by an administrator a notification identifying the file (column 6, lines 54-65).

Regarding claims 8, 21 and 34, Smithson teaches if the weighting indicates that the file is safe, said action performing code is operable to generate for access by an administrator a

notification identifying the file (column 8, lines 54-60 i.e. notification will be sent to administrator).

Regarding claims 9, 22 and 35, Chess discloses wherein if it is determined that a file sent to the computer is not currently entered in the statistical log (Figure 3A [block 301]), the logging code is further operable to create an entry in the statistical log for the file (column 5, lines 11-20), in which the value of said one or more predetermined attributes relating to the file are stored, and in which the count value is initialized (column 5, lines 1-5, column 5, lines 20-29).

Regarding claims 10, 23 and 36, Chess discloses wherein upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the statistical log to be incremented to account for the current occurrence of the file (column 2, lines 44-51, column 4, line 62 through column 5, line 5).

Regarding claims 11, 24 and 37, Smithson discloses reviewing files included in e-mail communications (column 3, lines 26-33), and each entry in the statistical log is further arranged to identify, for each sender of that file, the number of times that that sender has sent the file in addition to the count value indicating the total number of times that the file has been sent (column 4, lines 25-40).

Regarding claims 12, 25 and 38, Chess discloses discloses upon receipt of a file, the statistical log interface code is operable to cause the count value within the relevant entry of the

statistical log to be incremented to account for the current occurrence of the file (column 3, lines 17-23), and the number by which the count value is incremented is dependent on the number of times that the sender of the current occurrence of the file has previously sent that file (column 5, lines 1 1-28).

Claims 3-6, 13, 16-19, 29-32 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chess in view of Smithson, and further in view of U.S. Patent No. 6,401,210 to Templeton.

Regarding claims 3, 16 and 29, Chess discloses if the weighting indicates that the file is probably malware, said action performing code is operable to perform the steps of: notifying the user of the file (column 6, lines 51-62).

The combination of Chess and Smithson does not disclose encrypting the file such that only an administrator can decrypt that file.

Templeton discloses a method for managing virus-infected files (See Abstract) where he teaches detecting a virus in a file encrypting the file in such a way that only the administrator (system operator) can decrypt that file (column 3, lines 23-27, column 4, line 64 through column 5, line 5).

It would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Chess and Smithson with the teachings of Templeton to encrypt the file after detecting a virus present in the file in was that only the administrator can decrypt the file. One would be motivated to do so in order enable the system to safely store files that have a high probability of being infected and prevent the user from opening the files and

spreading the virus to another files or computers while being able to reproduce the original file for further analysis or cleaning at later time (column 1, lines 44-54).

Regarding claims 4, 17 and 30, Templeton discloses associating a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted (column 3, lines 61-64, column 4, lines 29-40).

Regarding claims 5, 18 and 31, Chess teaches notifying the user of the file (column 6, lines 51-62).

The combination of Chess and Smithson does not disclose encrypting the file such that only an administrator and the originator of the file can decrypt that file.

Templeton discloses a method for managing virus-infected files (See Abstract) where he teaches upon detecting a virus in a file encrypting the file (column 4, line 64 through column 5, line 5) in such a way that only the system operator or the owner can decrypt that file (column 3, lines 23-27, column 3, lines 50-55).

It would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Chess and Smithson with the teachings of Templeton to encrypt the file after detecting a virus present in the file in was that only the administrator or the owner can decrypt the file. One would be motivated to do so in order enable the system to safely store files that have a high probability of being infected and prevent the recipients from opening the files and spreading the virus to another files or computers while being able to reproduce the original file for further analysis or cleaning at later time (column 1, lines 44-54).

Regarding claims 6, 19 and 32, Templeton discloses wherein the action performing code is further operable to associate a message with the file for reference by a person receiving that file, the message identifying that the file has been encrypted (column 3, lines 61-64, column 4, lines 29-40).

Regarding claims 13, 26 and 39, Smithson discloses wherein if said action performing code is arranged, dependent on the weighting (column 5, line 65 through column 6, line 3), to quarantine the file or delete it.

The combination of Chess and Smithson does not disclose encrypting the file and an automated decryption code operable, if the file is subsequently determined to be safe, to perform the steps of: locating all encrypted occurrences of that file on a file system, and decrypting each said occurrence.

Templeton discloses a method for managing virus infected files (See Abstract) where he teaches after determining that a file has been infected (column 4, lines 44-45), encrypting that file for later time (column 4, lines 64-67) and when a determination is made that the file is safe to locate the file and decrypt each occurrence of that file (column 5, lines 16-31).

It would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the system to include locating and decrypting files that have been determined to be safe. One would be motivated to do so to enable the user to view and use files that have been analyzed and determined to be free from viruses.

(10) Response to Argument

In response to appellant's arguments regarding the rejection of claims 1-13 under 35 U.S.C. 101, the recitation "operating a computer to review files for potential malware" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

In response to Appellant's arguments that reciting "operating a computer to review files for potential malware" and stating that the code is "operable" after the function recite a functional set of acts being performed, the Examiner disagrees. The plain meaning of the term "operable" as understood by the Examiner means "capable of being put into use, operation or practice" (taken from <http://www.dictionary.com>). The Appellant never states that the code is running or executing, but merely that there is a possibility that the code or logic may be executed. The Examiner interprets the limitations of claims 1-13 and 27-39 as representing a computer listing *per se* that is capable of being executed, but never actually implemented, thereby representing non-statutory subject matter.

For the reasons stated above the rejection of claims 1-13 and 27-39 under 35 U.S.C. 101 should be maintained.

In response to the Appellant's arguments that neither of the cited references discloses logging code operable to maintain a statistical log having an entry for each file sent to the

computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file, the Examiner disagrees. As cited in the Office Action of 18 January 2006, and again above, the Examiner used *Chess* to reject the abovementioned limitation. *Chess* discloses in the various cited portions a database of document information (Figure 2 [block 204], column 4, lines 22-61) that maintains an entry for every file on the computer. *Chess* further goes on to states that the database can maintain a number of times the document has been reviewed for changes (column 4, line 62 to column 5, line 5).

It is held that *Chess* discloses logging code operable to maintain a statistical log having an entry for each file sent to the computer for review, each entry being arranged to store a count value indicating the number of times that the file has been sent to the computer for review and a value of one or more predetermined attributes relating to the file, and the rejection should be upheld.

In response to the Appellant's argument that the cited references does not disclose that the weighting would indicate the likelihood that a file has a value of one or more predetermined attributes will be malware and referencing the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with the file in the statistical log, the Examiner disagrees. *Smithson* was used to reject the limitation weighting would indicate the likelihood that a file has a value of one or more predetermined attributes will be malware as cited in the previous Office Action, and again above. *Smithson* teaches various parameters are measured and compared to threshold levels, and if the parameters exceed the threshold levels set forth than that file contains malware, see, for example,

column 4, lines 5-20. As discussed in the previous Office Action, *Smithson* discloses the weighting table, while *Chess* recites the statistical log. As mentioned above *Smithson* discloses a weighting table to determine a weighting associated with the file, as seen, for example in column 4, lines 5-20 in the discussion of exceeding various measurement parameters and exceeding certain thresholds. *Chess* discloses determining the likelihood of a document being infected with a virus based on data stored in the document information database, as seen in the citation above, and in the previous Office Action, of column 4, line 62 to column 5, line 5.

The combination of *Chess* and *Smithson* teaches the weighting would indicate the likelihood that a file has a value of one or more predetermined attributes will be malware and referencing the weighting table to determine the weighting to be associated with the file, based on the value of said one or more predetermined attributes associated with the file in the statistical log and the rejection should be sustained.

In response to the Appellant's argument that *Chess* does not disclose a statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file, the Examiner disagrees. As cited above and in the previous office action at column 5, lines 11-16, *Chess* states that the document database disclosed above is consulted for each document, thereby providing for sometime of interface for the database. As discussed above, *Chess* discloses maintaining a count value in the database.

Chess teaches a statistical log interface code operable, upon receipt of a file, to determine with reference to the statistical log the count value relating to that file and as such the rejection should be maintained.

In response to appellant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In response to appellant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, *Smithson* provides for motivation to combine the references at column 2, lines 10-15 stating that the combination provides for a method to detect unknown viruses more readily, thereby preventing infection of computer systems.

In response to the Appellant's argument that the cited references do not identify the number of times a particular sender transmits the same file, the Examiner disagrees. The Examiner agrees that *Smithson* does not explicitly state a number of times a sender transmits a file. *Smithson* provides examples of various measurement parameters that can be arranged by a system-manager. As admitted by the Appellant, *Smithson* teaches wherein a number of times a file is sent is tracked. One of ordinary skill in the art would recognize that it would be simple to modify the example rules outlined in *Smithson* to track the number of times a particular sender transmits the same file. The Appellant is reminded that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary

reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Applicant's arguments regarding the rejection of claims 2-6, 13, 16-19, 26, 29-32 and 39 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

This examiner's answer contains a new ground of rejection set forth in section (9) above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte dismissal of the appeal* as to the claims subject to the new ground of rejection:

(1) Reopen prosecution. Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) Maintain appeal. Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

Christian LaForgia 
Patent Examiner
Art Unit 2131


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

James Dwyer
Director
Technology Center 2100

Conferees:

Gilberto Barron 
Supervisory Patent Examiner
Art Unit 2132

Application/Control Number: 10/028,906
Art Unit: 2131

Page 17

Matthew Smithers 
Primary Examiner
Art Unit 2137